MQ Auditor Overview

- MQ Auditor (MQA) allows a company to audit / track all MQ API calls performed by MQ applications (local & remote) that are connected to a queue manager.
- The API Exit operates with IBM MQ v7.0, v7.1, v7.5, v8.0, v9.0 & v9.1 in Windows, Unix, IBM i and Linux environments.
- It is designed to provide the user with all of the information of an MQ API call in "human readable" format.
- It will convert Command Server / PCF messages into human readable messages.
What’s new in MQ Auditor v3.0.0

- Added Topics keyword to control what topics will be audited.
- Added UseExcludeTopics and ExcludeTopics keywords to explicitly exclude topics from being audited.
- Enhanced the processing for Subscriptions.
- Fixed an issue with large usr folder for an MQRFH2 (JMS) message.
- Fixed an issue with formatting of some MQCHARV fields for MQSD structure.
- Fixed an issue with MQPut1 using the correct audit file.
- Fixed an issue with PMO ‘NewMsgHandle’ string being in the wrong location.
- Fixed an issue with determining the application name.
- Fixed an issue with PCF messages (>10KB) being converted to human-readable.
- Fixed an issue with PCF messages not being handled for MQCALLBACK.
Trackable MQ API Calls

- V6 & lower MQ API calls: MQCONN, MQCONNX, MQOPEN, MQGET, MQPUT, MQPUT1, MQINQ, MQSET, MQCLOSE, MQDISC, MQBACK, MQBEGIN and MQCMIT.

- MQ API calls added in MQ v6.0.2.7: XASTART, XAEND, XAOPEN, XACLOSE, XACOMMIT, XACOMPLETE XAFORGET, XAPREPARE, XARECOVER, XAROLLBACK, AX_REG and AX_UNREG.

- MQ API calls added in MQ v7: MQCALLBACK, MQCB, MQCTL, MQSTAT, MQSUB and MQSUBRQ.
Trackable MQ Structures

- V6 & lower: MQCNO, MQOD, MQGMO, MQPMO and MQMD.
- Embedded MQ structures: MQCIH, MQDH, MQDLH, MQIIH, MQRFH, MQRFH2, MQRMH, MQTM, MQWIH, MQXQH, MQHSAP & SMQBAD.
- Since MQ v7: MQCBC, MQCBD, MQSTS and MQSD.
MQ Auditor Audit Files

- The output (audit) information is written to plain text CSV (Comma Separate Value) files.

- There are 2 Audit CSV file types:
  - *Queue Manager Audit* file contains information for MQCONN/X, MQDISC, MQOPEN, MQCLOSE, MQCMIT, MQBACK, etc...
  - *Queue/Topic Audit* file contains information for MQGET, MQCALLBACK, MQPUT, MQPUT1, MQINQ and MQSET.
MQ Auditor Audit Record to a Queue

- The user can choose to have the output (audit) information written to a *local* or *remote* queue rather than to a file.

- If the audit data is written to a queue then this action can potentially cause an endless loop (MQA will audit itself, over and over again). Therefore, the "audit queue" is not audited / monitored nor is the transmit queue if remote queue is used.

- If the user is using a remote queue then it is strongly recommended that a separate channel and transmit queue be used so that the normal transmit queue can be audited / monitored.

- The user will need a program to read the messages from the 'audit queue' and write the information somewhere (i.e. DB).
MQ Auditor Audit Files

- The user can choose to have the output (audit) information written to a local or remote queue rather than to a file.

- Use *Audit Queue Off Load* (AQOL) on a different queue manager to collect and write audit records to audit files.

- You can deploy MQA to 20 queue managers who all send their audit records to a single (different) queue manager where AQOL collects and writes audit records to audit files.
Audit Queue Off Load
Queue Manager Audit File

2014/09/25 18:01:24.037716, MQXF_CONNX, A, PID=12612, TID=7, CC=0, RC=0, UserId=MUSR_MQADMIN, HConn=20971533, QMgrName=MQWT2, CNO_Options=MQCNO_HANDLE_SHARE_BLOCK+MQCNO_SHARED_BINDING+MQCNO_RECONNECT_AS_DEF, SecurityId=1D010105000000000000515000000FAE66C00D5EA80C2BF2341ACF2030000000000000000000000000000000, PgmName=Sphere MQ\bin64\amqrmppa.exe, PgmType=MQXACT_EXTERNAL, Env=MQXE_MCA_SVRCONN

2014/09/25 18:01:24.047716, MQXF_OPEN, A, PID=12612, TID=7, CC=0, RC=0, UserId=tester, HConn=20971533, HObj=4, ChannelName=SYSTEM.DEF.SVRCONN, ConName=127.0.0.1, LongRemoteUserId=tester, MCAUserIDLong=tester, SecurityId=1D010105000000000000515000000FAE66C00D5EA80C2BF2341ACEE0300000000000000000000000000000000, OpenOptions=MQOO_BIND_AS_Q_DEF+MQOO_INQUIRE+MQOO_FAIL_IF_QUIESCING, OD_ObjType=MQOT_Q, OD_ObjName=TEST.Q1, OD_DynamicQNames=AMQ.*, OD_ResolvedQMgrName=MQWT2, OD_ResolvedQName=TEST.Q1

2014/09/25 18:01:24.047716, MQXF_INQ, A, PID=12612, TID=7, CC=0, RC=0, UserId=tester, HConn=20971533, HObj=4, SelectorCount=5, Selectors=MQIA_COMMAND_LEVEL+MQIA_PLATFORM+MQIA_CODED_CHAR_SET_ID+MQCA_Q_MGR_NAME+MQCA_Q_MGR_IDENTIFIER, MQWT2

2014/09/25 18:01:24.147716, MQXF_CLOSE, A, PID=12612, TID=7, CC=0, RC=0, UserId=tester, HConn=20971533, HObj=-1, CloseOptions=MQCO_NONE,

2014/09/25 18:01:24.147716, MQXF_CMIT, A, PID=12612, TID=7, CC=0, RC=0, UserId=tester, HConn=20971533

2014/09/25 18:01:24.147716, MQXF_DISC, A, PID=12612, TID=7, CC=0, RC=0, UserId=tester, HConn=20971533
Queue Audit File

2014/09/25 18:01:24.077716, MQXF_PUT, A, PID=12612, TID=7, CC=0, RC=0, Userld=tester, HConn=20971533, HObj=4, PMO_Options=MQPMO_NO_SYNCPOINT+MQPMO_SYNC_RESPONSE+MQPMO_RESPONSE_AS_Q_DEF+MQPMO_RESPONSE_AS_TOPIC_DEF, PMO_ResolvedQMgrName=MQWT2, PMO_ResolvedQName=TEST.Q1, MD_PutDate=2014/09/25, MD_PutTime=22:01:24.04, MD_MsgId=414D51204D51413120202020202020201DB6094120000501, MD_Format=MQSTR, MD_MsgType=MQMT_DATAGRAM, MD_Persistence=MQPER_NOT_PERSISTENT, MD_ReplyToQMgr=MQA1, MD_UserId=tester, BufferLength=23, MsgData=This is test message #1

2014/09/25 18:01:24.077716, MQXF_PUT, A, PID=12612, TID=7, CC=0, RC=0, Userld=tester, HConn=20971533, HObj=4, PMO_Options=MQPMO_NO_SYNCPOINT+MQPMO_SYNC_RESPONSE+MQPMO_RESPONSE_AS_Q_DEF+MQPMO_RESPONSE_AS_TOPIC_DEF, PMO_ResolvedQMgrName=MQWT2, PMO_ResolvedQName=TEST.Q1, MD_PutDate=2014/09/25, MD_PutTime=22:01:24.07, MD_MsgId=414D51204D51413120202020202020201DB6094120000502, MD_Format=MQSTR, MD_MsgType=MQMT_DATAGRAM, MD_Persistence=MQPER_NOT_PERSISTENT, MD_ReplyToQMgr=MQA1, MD_UserId=tester, BufferLength=23, MsgData=This is test message #2
MQ Auditor Secondary Features

- The user can define 4 types of filters: Applications, UserIDs, Queues & Topics

- **One File Per Connection** will cause MQA to output all audit information to the Queue Manager Audit file (the Queue Audit file will not be used).

- **Shared Queue Audit File** will cause MQA to output all audit queue information to a single Queue Audit file.

- **Use Rolling Audit File** enables MQA to manage of the Audit (QMgr and Queue) file size.
MQ Auditor Secondary Features

- MQA will automatically archive Audit files to an archive directory. The number of days for saved archived Audit files is 7.
- Explicitly exclude queues from being monitored.
- Explicitly exclude topics from being monitored.
- Explicitly exclude UserIDs from being monitored.
- The user can select to not have audit information written for particular reason codes (i.e. 2033).
MQ Auditor IniFiles

- MQ Auditor use an initialization files (IniFile) to configure how the API exit is to run.
- One IniFile is used for each queue manager.
- MQ Auditor has a large number of keywords and values that can be used. Hence, it is best to use the MQA-GUI to update the values for keywords.
MQ Auditor IniFile

```
[default]
Active=Y
LogMode=N
LogFile=C:\capitalware\MQA\mqaq.log
#
MonitorType=A
MsgDataAsHex=N
MsgDataLength=-1
AuditFileMaxSize=400
UseRollingAuditFile=Y
OneFilePerConnection=N
SharedQueueAuditFile=Y
StartupCleanup=N
ArchiveCleanup=Y
ArchiveDays=14
MonitorInternal=N
#
ShowAPI=MQGET;MQCALLBACK;MQPUT;MQPUT1
###ShowAPI=MQGET; MQCALLBACK; MQPUT; MQPUT1; MQOPEN; MQDISC; MQCLOSE; MQCONN; MQCONN
#
ShowCNO = Options; SSLConfigPtr; SecurityParmsPtr
ShowGMO = MatchOptions; Options; ResolvedQName; WaitInterval
ShowPMO = Options; ResolvedQMgrName; ResolvedQName
ShowMD=PutDate; PutTime; MsgType; Format; Persistence; MsgId; CorrelId; ReplyToQ; ReplyToQMgr; UserId
#
UseExcludeQueues=Y
ExcludeQueues=AMQ* ; SYSTEM* ; MQMON* ;
```
MQA IniFile Configuration via MQA-GUI
MQA IniFile Configuration via MQA-GUI
MQA IniFile Configuration via MQA-GUI
MQA IniFile Configuration via MQA-GUI
MQA IniFile Configuration via MQA-GUI
MQA IniFile Configuration via MQA-GUI
MQA IniFile Configuration via MQA-GUI
Questions & Answers